ZyXEL

ZyXEL

Vantage Report

3.0.05.61.00

Release Note

Date: 11/02/2006

1 Supported Platforms

- **Vantage Report 3.0.05.61.00 Environment Requirement:**

1.1 Hardware platform:

Server Requirements:

The number of the registered devices	CPU Spec (GHz)	Memory Spec (GB)	Free Hard Disk Spec (GB)	The speed of receiving logs
<5	Intel P4 2.6	1	10	<=1500 logs/sec
<50	Intel P4 2.6	1	Device number *2	<=1500 logs/sec
50-100	Intel P4 3.2 +	1	Device number *2	<=1500 logs/sec

Client Requirements:

CPU: Intel P3 450 MHz or better

1.2 Software environment:

Server: Windows XP Professional, Windows 2000/2003 Server.

Client: Microsoft IE 6.0 or later, Firefox 1.0.7 or later, Mozilla 1.7.12 or later on Microsoft Windows Platform.
Screen resolution supported: 1024*768

Other system services such as SMTP daemon are also needed for Vantage Report featured services.

2 Version

Vantage Report 3.0.05.61.00.

3 Features

Main features

- **Dashboard**

  Provide a quick and top level summary of activity of firewalls. Giving options to easily drill down to generate instant reports and log viewer for viewing events of interest.

- **Monitor**

Including bandwidth monitor, service monitor, attack monitor, intrusion monitor, anti-virus monitor and anti-spam monitor.

- **Traffic Report**
  - **Bandwidth Usage Report**
    Including summary report, top protocols report, top hosts report, top users report and top destinations report.
  - **WEB Traffic Report**
    Including top sites report, top hosts report and top users report.
  - **FTP Traffic Report**
    Including top sites report, top hosts report and top users report.
  - **MAIL Traffic Report**
    Including top sites report, top hosts report and top users report.
  - **Customization Service Traffic Report**
    Including customizing services, top sites report, top hosts report and top users report.
- **VPN Report**
  - **Site-to-Site Report**
    Including link status report, traffic monitor, top peer gateways report, top sites report, top tunnels report, top protocols report, top hosts report, top users report and top destinations report.
  - **Remote Access Report**
    Including total users & traffic monitor, user status report, top protocols report and top destinations report.
  - **Xauth**
    Show successful xauth login events and failed xauth login events.
- **Network Attack Report**
  - **Attack Report**
    Statistics of all attacks, including summary report, top attacks report, top sources report, and type report.
  - **Intrusion Report**
    Statistics of all intrusions, including summary report, top intrusions report, top sources report, top destinations report and severity report.
  - **Anti-Virus Report**

    Statistics of all virus infections, including summary report, top viruses report, top sources report and top destinations report.
  - **Anti-Spam Report**

    Statistics of all spam mails, including summary report, top senders report, top sources report and score report.
- **Security Policy Report**
  - **Firewall Access Control Report**

    Statistics of the blocked packets, including top users blocked report and top packets blocked report.
  - **Application Access Control Report**

    Statistics of the connections that users access applications, including top applications blocked report, top users blocked report and top applications allowed report.

- **WEB Blocked Report:**

  Statistics of the attempts that users made to access blocked sites, including summary report, top sites report, top hosts report, top users report and category report.

- **WEB Allowed Report:**

  Statistics of the attempts that users made to access forwarded sites, including summary report, top sites report, top hosts report and top users report.

➢ **Event**

- **Device Login**

  Show successful login events and failed login events.

- **Sessions Per Host**

  Statistics of the occurrences that users exceed the max sessions, including top hosts report and top users report.

➢ **Log viewer**

Including the query to general logs and the query to critical logs.

➢ **Schedule Reports**

- **Summary**

  Including weekly report, daily report and overtime report.
- **Template**
  Users can define own templates and apply them their schedule reports.

➢ **Log Receiver Monitor**
Monitoring the number of the logs received by VRPT.

What's New (vs. VRPT 2.3.1)

➢ **Support ZyWALL 1050**

Provide full support for ZyWALL 1050.

➢ **Dashboard**

Provide a quick and top level summary of activity of firewalls. Giving options to easily drill down to generate instant reports and log viewer for viewing events of interest.

➢ **Template for scheduled customized report**

Users can define own templates and apply them to their schedule reports.

➢ **Log Viewer for reports**

When generating a report online, users can look up the raw logs related to the report through the "View Logs" icon.

➢ **Reverse local IP to hostname**

Reverse local IP address to hostname.

4 Notes

1. Following is the list of devices and their firmware versions supported:

Vantage Report 3.0 Test Matrix	Vantage Report 3.0 Supports Device F/W
ZW 2/10W	3.62
ZW 5/35/70	3.62, 3.63, 3.64, 4.00 and later
ZW P1	3.64 and later
Prestige 662/652	3.40
IDP 10	2.00
ZW 1050	1.01

2. If VRPT 2.3 has been installed in your system, please upgrade VRPT2.3 to VRPT2.3.1 first. The VRPT 3.0 installation package will detect installed VRPT 2.3.1 automatically and notice you to upgrade from 2.3.1 to 3.0.
   If VRPT 2.2 has been installed in your system, please uninstall it first.

3. VRPT 3.0 is very sensitive to the system time. Please make sure the system time is correct and do not change the system time while VRPT is running.

4. VRPT 3.0 uses Macromedia's Flash to display the graphics. You will be asked to install the Flash player if it is not present.

5. The administrator's initial account is root/root. After installing VRPT 3.0, please access http://<vrpt host>:<port>/ to login VRPT 3.0. You should change the password for root account and configure the mail server through System>Server Configuration.
   If you installed VRPT 2.3.x series before, please clear the cached files in the browsers before accessing VRPT 3.0. Please reference Appendix B to get the operations.

6. If there are too many records in your database, it will take longer time to display the statistics.

7. The port number used in VRPT 3.0 standalone.

Port	Protocol	Comment
3316	TCP	Used by MySQL
Configurable (default 8080)	TCP	HTTP service.
514	UDP	Syslog Daemon

8. VRPT logs the quantity of the received logs for every registered device, unregistered device. VRPT also logs the quantity of the logs that can't be parsed. You can find the log files in <VRPT_Home>/vrpt/log folder. The filename for current day is LogRecord.log. And filename of history files is LogRecord.log_yyyy-mm-dd. You can reference Appendix A to get the format in the files.

5 Known Issues

1. All Firefox browser instances on a machine share one session, so VRPT allows to be accessed by only one Firefox browser instance. The same is true for Mozilla.
   IE does not have this restriction since each IE has its own session.
2. The print function is not available in Firefox browser.
3. In schedule report template, the .jpg and .gif files are allowed as template logo files. But the .jpg files are recommended.

6 Changes

[ENHANCEMENT]

Add Security Policy->Firewall Access Control report and Event->Sessions Per Host report.

[ENHANCEMENT]
Add “Dropped Log” attribute in Log Record.

[ENHANCEMENT]
Beautify the monitor flash and report flash.

[CHANGE]
Attack category for ZyWALL series (except ZyWALL 1050) is changed.
In VRPT 2.3.x, if msg is one of the following:

- land TCP
- land UDP
- land IGMP
- land ESP
- land GRE
- land OSPF

The attack category will be counted as “land [TCP | UDP | IGMP | ESP | GRE | OSPF]”

It is the same to “ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]” or “ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]”

In VRPT 3.0, if the msg is one of previous list, then it is counted as an attack. For example, the msg is “lan TCP”, the attack is “land TCP”.

For reports on GUI for ZyWALL series (except ZyWALL 1050), there are following reports for attack.

- Summary -> Attack
- Top Attacks -> Source
- Top Sources -> Attack

[CHANGE]
The drill down report for VPN ->Site to Site -> Top Host report is changed. The drill down report for VPN ->Site to Site -> Top Host report in VRPT 2.3.x is Top Peer Gateways. In VRPT 3.0, the drill down report for VPN ->Site to Site -> Top Host report is Top protocols.

[CHANGE]
The Traffic->MAIL->Top Sites report only retrieves the traffic logs that have SMTP protocol. The Traffic->MAIL->Top Hosts report and Traffic->MAIL->Top users report only retrieve the traffic logs that have POP3 protocol.

[CHANGE]
Add source IP column in authentication list.

[CHANGE]
The bandwidth statistics of the bandwidth monitor is changed.
In VRPT 2.3.x, the total amount of traffic handled by the selected device in a minute is shown.
In VRPT 3.0, the bandwidth (KBytes/s, the average in a minute) is shown.

Appendix A

The log format in LogRecord.log

We explain the log format in LogRecord.log file through examples.

Time: 2005-12-26 02:49:11, MAC: 00A0C5123410, Log Amount: 1, Attribute: First log/Registered

This log means VRPT receive the first log at 2005-12-26 02:49:11 for the device whose MAC is 00A0C5123410 since VRPT starting up. And the device is registered in VRPT.

Time: 2005-12-26 02:49:12, MAC: 00A0C5123411, Log Amount: 1, Attribute: First log/Unregistered

This log means VRPT receive the first log at 2005-12-26 02:49:12 for the device whose MAC is 00A0C5123411 since VRPT starting up. And the device is unregistered in VRPT.

Time: from 2005-12-26 02:49:11 to 2005-12-26 02:54:11, MAC: 00A0C5123410, Log Amount: 58, Attribute: Registered

This means VRPT receive 58 logs from 2005-12-26 02:49:11 to 2005-12-26 02:54:11. The device MAC is 00A0C5123410. And the device is registered in VRPT.

Time: from 2005-12-26 02:49:11 to 2005-12-26 02:54:11, MAC: 00A0C5123411, Log Amount: 58, Attribute: Unregistered

This means VRPT receive 58 logs from 2005-12-26 02:49:11 to 2005-12-26 02:54:11. The device MAC is 00A0C5123411. And the device is unregistered in VRPT.

Time: from 2005-12-27 09:46:27 to 2005-12-27 09:51:27, MAC: , Log Amount: 8, Attribute: Can not be parsed

This means VRPT receive 8 logs that can't be parsed from 2005-12-27 09:46:27 to 2005-12-27 09:51:27. These logs may be sent by non-ZyXEL devices or sent by hackers.

Time: from 2005-12-26 02:49:11 to 2005-12-26 02:54:11, MAC: 00A0C5123411, Log Amount: 58, Attribute: Dropped log

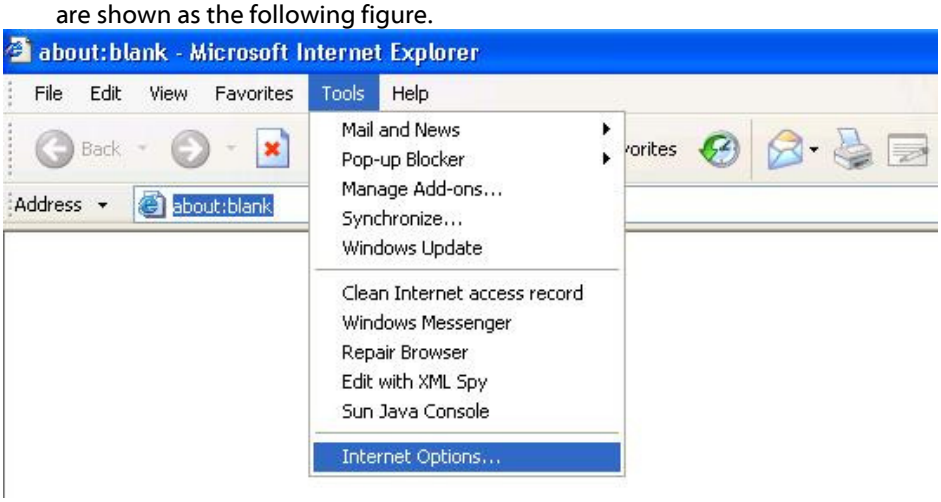
This means VRPT receive 58 logs from 2005-12-26 02:49:11 to 2005-12-26 02:54:11. The device MAC is 00A0C5123411. And the logs are dropped because the total logs of the device in the database are more than the maximum allowed.

Appendix B

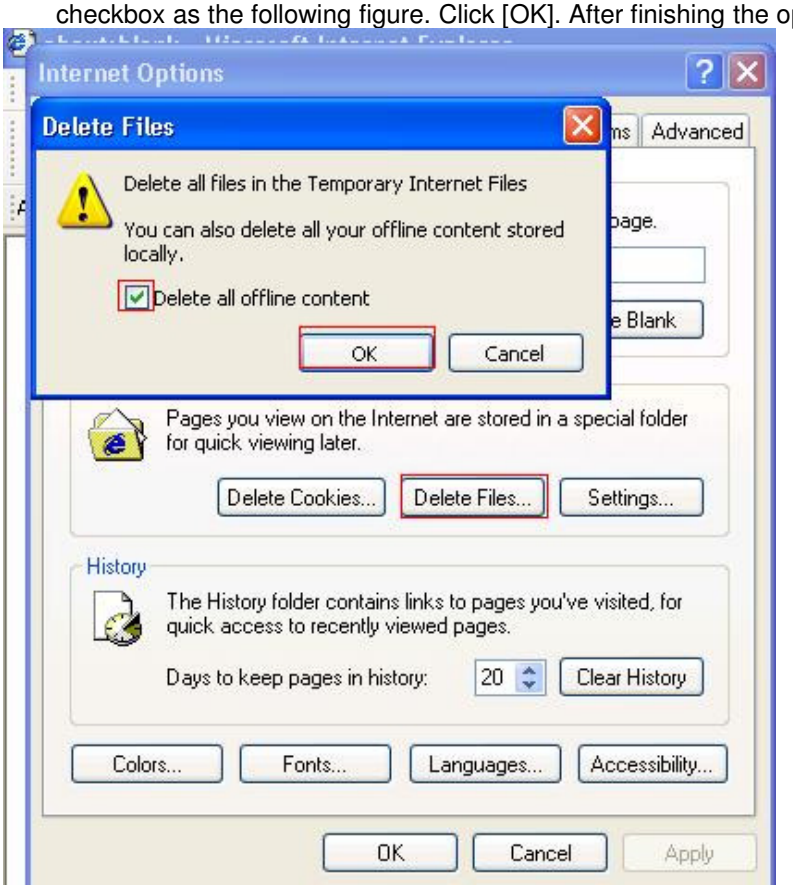
The operations of cleaning the cached files in browser

IE Browser

1. Open a IE browser, click [Tools]->[Internet Options] to open Internet Options dialog. The operations are shown as the following figure.

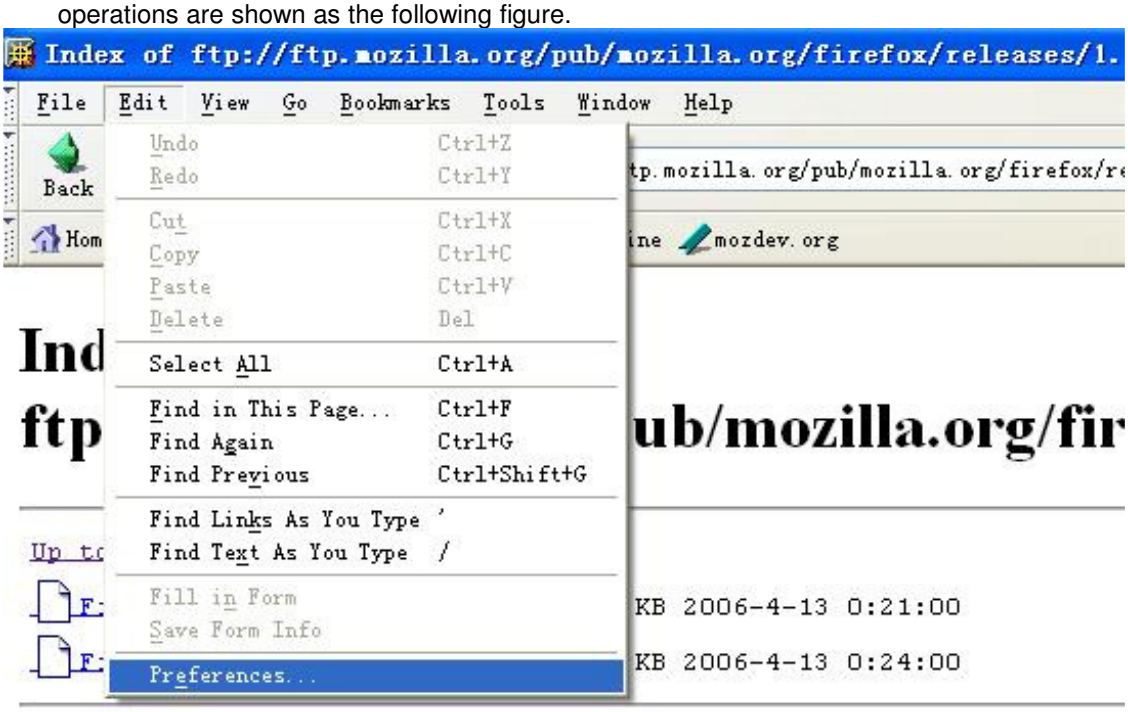


2. In Internet Options dialog, click [Delete Files…] button to open Delete Files dialog, check the checkbox as the following figure. Click [OK]. After finishing the operations, close the dialog.

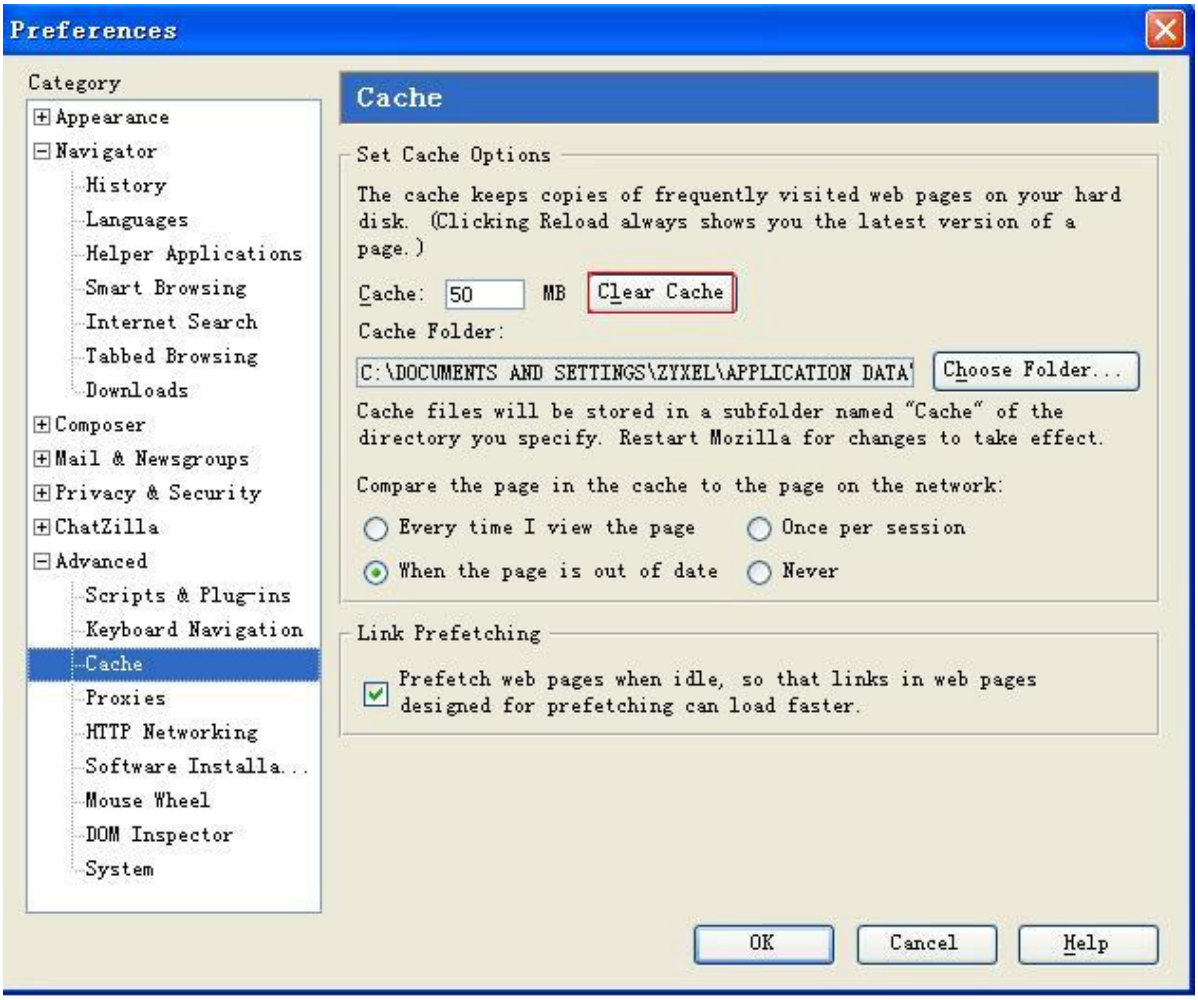


Mozilla Browser

1. Open Mozilla browser, click [Edit] -> [Preferences…] to open the Preferences window. The operations are shown as the following figure.



2. The Preferences window is shown as the following. Click [Advanced] -> [Cache] -> [Clear Cache]. After finishing these operations, close the window.



Firefox Browser

1. Open Firefox browser, click [Tools] -> [Options…] to open the Options window. The operations are shown as the following figure.

2. The Options window is shown as the following figure. Click [Privacy] -> [Clear] in red rectangle. After finishing these operations, close the window.